THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 3

The weight of security: measuring the benefits of robust encryption

PROMPT

Some justify invasive surveillance techniques and authorities by pointing to terrorist attacks, injuries, and deaths. However, encryption also saves lives. This side of the scale, favoring robustly secured networks, is not well defined. This track will explore the benefits — including the return on investment — of encryption and try to formulate a means to quantify and measure those benefits.

DISCUSSION LEADERS

Harlo Holmes,
Freedom of the Press Foundation

Eva Galperin, EFF

WORKSHOP LEADERS

Morgan Marquis-Boire,
First Look Media

Riana Pfefferkorn, Stanford CIS

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

Key Outcome: Compiled narrative stories which attempt to quantify the value of encryption, predicted next stage of debate, and proposed several counter-narratives and talking points.

MEASURING BENEFITS OF ENCRYPTION, IN REVERSE

Finding stories where encryption prevented negative results is difficult — you cannot prove the negative. The best example we have is that mobile device encryption, particularly coupled with a remote-wipe feature, ensures that a person's information stored on their phone cannot be exploited if their phone is stolen (such as by accessing sensitive information in email, or calling the person's contacts to demand money). Therefore, the group examined where the failure to use encryption, to use encryption properly, or to understand the undisclosed limitations of an encryption tool, led to increased risk to the user, or worse, actual harm.

The group discussed use cases where encryption tools or systems did not behave as expected, or where differing levels of security were not presented transparently, leaving the user with a false sense of security. This could be because the program did not behave as it said it would. Encryption systems may fail open instead of closed, defaulting to sending a message unencrypted (unbeknownst to the user). In the Windows desktop version of PGP, the program sends unencrypted email even when its UI indicates the opposite. Also, Telegram poorly mixes and matches encrypted and unencrypted conversations non-transparently, despite its reputation as a secure tool; poor UI creates the opportunity for a mismatch in user expectations.

This user expectation mismatch may also occur because the user did not understand the program's limitations. Protonmail users may falsely think that their messages are safe no matter whom they're emailing, when this is not the case when it comes to messages exchanged with non-Protonmail accounts. Somewhat relatedly, FBI investigators were able to access Gen. Petraeus's Gmail account and read the messages he was exchanging with his biographer/mistress in their shared account's unsent drafts folder.

Another issue is when an "encrypted" messaging program nevertheless keeps messages readable to the provider on the server, such that a user may be at risk of disclosure by the company of plaintext to the user's government. Egyptian police interrogated an arrestee and read the arrestee's Skype communications

THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 3

The weight of security: measuring the benefits of robust encryption

PROMPT

Some justify invasive surveillance techniques and authorities by pointing to terrorist attacks, injuries, and deaths. However, encryption also saves lives. This side of the scale, favoring robustly secured networks, is not well defined. This track will explore the benefits — including the return on investment — of encryption and try to formulate a means to quantify and measure those benefits.

DISCUSSION LEADERS

Harlo Holmes,
Freedom of the Press Foundation

Eva Galperin, EFF

WORKSHOP LEADERS

Morgan Marquis-Boire,
First Look Media

Riana Pfefferkorn, Stanford CIS

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

to them, when the arrestee had relied upon Skype to securely encrypt those messages. The arrestee, like many Skype users, may not have known that Microsoft retains the capability to scan the plaintext of messages. Microsoft's escrow of users' keys and retention of message contents is not well-known, and while the company does refuse to give information to some governments, it provides data to many others — something users can only learn about if the company discloses it honestly and accurately in its transparency report. Skype illustrates the importance of provider transparency to users about how their systems work and how they cooperate with legal authorities around the world.

The group discussed UI changes as a way of better notifying people about the nature and limitations of the security of the systems they use, to make it clear when messages are not encrypted or indicate differing levels of security for different conversations within the same tool or system. For example, Gmail now provides UI indicators about TLS support for both incoming and outgoing email.

The group also touched upon suspicions of monitoring that have been shared in digital security workshops that some participants had conducted or attended, such as strange beeping noises on a phone line thought to be secure, or home visits by police even after using a tool thought to be secure.

The group discussed other vectors for compromise besides user-side failure to properly configure and use encryption, or provider-side failure to accurately communicate how the system works. For example, Access Now noted a pattern of numerous complaints from Latin America of being compromised via malware; investigation revealed consistent malware infection on compromised devices, which is suspected to originate from a South American state actor. Additionally VPNs can be compromised by state actors. It is known that China degrades or blocks VPNs, and after it breaks one VPN, it then uses throttling/degradation to herd users onto broken VPNs.

Finally, the group discussed the importance of people who are not high-risk users using encryption for non-sensitive information or communications, in order to provide cover for those who have greater risk. This adds "noise" to the "signal" a targeted user sends by being the only one using encryption. For example, journalists in Turkey were arrested for use of "encryption" tools "linked to terrorists"; normalizing the use of those tools for everyday communications would make it harder for the state to paint all encryption users with the same "terrorist" brush, and would take away the justification for targeting journalists. Similarly, a different journalist chose not to file a story because one source was the only one at their organization using Signal, meaning they would stick out. Were Signal in greater use within the organization, the source could not be easily traced.

THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 3

The weight of security: measuring the benefits of robust encryption

PROMPT

Some justify invasive surveillance techniques and authorities by pointing to terrorist attacks, injuries, and deaths. However, encryption also saves lives. This side of the scale, favoring robustly secured networks, is not well defined. This track will explore the benefits — including the return on investment — of encryption and try to formulate a means to quantify and measure those benefits.

DISCUSSION LEADERS

Harlo Holmes,
Freedom of the Press Foundation

Eva Galperin, EFF

WORKSHOP LEADERS

Morgan Marquis-Boire,
First Look Media

Riana Pfefferkorn, Stanford CIS

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

THE NEXT STAGE OF DEBATE

The coalition in support of strong encryption is broad and robust. It includes technologists, security engineers, technology industry, civil libertarians, conservatives, and liberals. The strength of this coalition can be seen in the swift, public backlash against the Department of Justice in the "Apple vs FBI" case. Even during a compelling situation involving international terrorism on U.S. soil, polls consistently showed that critics of encryption were not able to gain ground. We predict that those working against strong encryption will change their tactics in an attempt to find "wedge" issues to fragment this coalition.

Currently, politicians and law enforcement frequently invoke worst-case scenarios that appeal to our sense of compassion rather than our sense of logic. We call these villains the Four Horsemen of the Apocalypse — terrorists, pedophiles, drug dealers, and kidnappers. Frequently these stories break down under logical scrutiny, but appeals to fears in a dangerous world clearly resonate with a large percentage of the population.

We postulate that U.S. President Obama's comments during South by Southwest might telegraph the next stage of debate. President Obama said, "If technologically it is possible to create an impenetrable device or system … then how do we apprehend the child pornographer? How do we disrupt a terrorist plot? What mechanisms do we have available to even do simple things like tax enforcement?" We suggest that President Obama, and the anti-encryption community in general, are not concerned about big banks and taxes in this context, but rather these are issues that might segment the coalition in support of strong encryption.

For example, if you explain to a civil libertarian that we must weaken encryption in order to investigate banking malfeasance and tax evasion, that might be compelling to some people. If it can be shown that big banks are avoiding regulatory bodies, that wealthy individuals are able hide financial assets, or that government employees are skirting open government regulations using secure, encrypted messaging tools, then some people might be convinced.

THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 3

The weight of security: measuring the benefits of robust encryption

PROMPT

Some justify invasive surveillance techniques and authorities by pointing to terrorist attacks, injuries, and deaths. However, encryption also saves lives. This side of the scale, favoring robustly secured networks, is not well defined. This track will explore the benefits — including the return on investment — of encryption and try to formulate a means to quantify and measure those benefits.

DISCUSSION LEADERS

Harlo Holmes,
Freedom of the Press Foundation

Eva Galperin, EFF

WORKSHOP LEADERS

Morgan Marquis-Boire,
First Look Media

Riana Pfefferkorn, Stanford CIS

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

NARRATIVES TO COUNTER NEW TALKING POINTS

Where logical arguments are the rock, we must expand to appeal to the "gut level feelings." Essentially, we need better stories. We need to go beyond technical arguments, and bring this debate home to family values.

Example One:

Everyone has a minority viewpoint in some context. The counter argument to allowing regulators access to any information any place it resides, is that the regulators themselves might go wrong. If you are an activist, in a sexual or religious minority, or part of a Tea Party nonprofit (to take some real-world examples), then you could be targeted.

Example Two:

We need to move away from talking about encryption in ones and zeros. Instead of talking about privacy, let's talk about intimacy. You may have nothing to hide, but you may not want to share your intimate moments.

Example Three:

Encryption is about family values. We, as a society, further public policy of family as a cohesive unit and promote trust and support within the family. We should promote the protections given to communications between spouses by making sure that people can communicate through encryption.

Example Four:

The internet of things connects your private spaces at home to the internet. Your baby monitor can be hacked by strangers. Your bedroom television can film you in your most intimate moments. Your home security system can capture you when you're sick and want to crawl away from the world. Your home is your sanctuary, and you shouldn't have to give up the benefits of modern living to achieve it.

This event is brought to you by accessnow

Access Now (accessnow.org) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, visit https://www.accessnow.org/crypto-summit-2-0/
or contact Nathan White (nathan@accessnow.org) & Amie Stepanovich (amie@accessnow.org)